PATENT COOPERATION TREATY

From the
INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

To:

KLETT, Peter M.
IBM Research GmbH
Zurich Research Laboratory
Saeumerstrasse 4 / Postfach
CH-8803 Rueschlikon
SUISSE

TERMIN: 5 June 2005

PCT

WRITTEN OPINION
(PCT Rule 66)

Date of mailing *(day/month/year)*	05.04.2005
Applicant's or agent's file reference: CH920030006	**REPLY DUE** **within 2 month(s)** from the above date of mailing

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/IB 03/05328	20.11.2003	30.05.2003

International Patent Classification (IPC) or both national classification and IPC
H04L29/06

Applicant
INTERNATIONAL BUSINESS MACHINES CORPORATION et al.

1. This written opinion is the **first** drawn up by this International Preliminary Examining Authority.

2. This opinion contains indications relating to the following items:

I	☒	Basis of the opinion
II	☐	Priority
III	☐	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
IV	☐	Lack of unity of invention
V	☒	Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
VI	☐	Certain documents cited
VII	☐	Certain defects in the international application
VIII	☐	Certain observations on the international application

3. The applicant is hereby **invited to reply** to this opinion.

When? See the time limit indicated above. The applicant may, before the expiration of that time limit, request this Authority to grant an extension, see Rule 66.2(d).

How? By submitting a written reply, accompanied, where appropriate, by amendments, according to Rule 66.3. For the form and the language of the amendments, see Rules 66.8 and 66.9.

Also: For an additional opportunity to submit amendments, see Rule 66.4. For the examiner's obligation to consider amendments and/or arguments, see Rule 66.4 bis. For an informal communication with the examiner, see Rule 66.6.

If no reply is filed, the international preliminary examination report will be established on the basis of this opinion.

4. The final date by which the international preliminary examination report must be established according to Rule 69.2 is: 30.09.2005

Name and mailing address of the international preliminary examining authority:

European Patent Office
D-80298 Munich
Tel. +49 89 2399 - 0 Tx: 523656 epmu d
Fax: +49 89 2399 - 4465

Authorized Officer
Kopp, K

Formalities officer (incl. extension of time limits)
Barrio Baranano, A
Telephone No. +49 89 2399-8621

WRITTEN OPINION International application No. PCT/IB 03/05328

I. Basis of the opinion

1. With regard to the **elements** of the international application *(Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this opinion as "originally filed")*:

Description, Pages

1-13 as originally filed

Claims, Numbers

1-22 as originally filed

Drawings, Sheets

1/4-4/4 as originally filed

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

   These elements were available or furnished to this Authority in the following language: , which is:

   ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).
   ☐ the language of publication of the international application (under Rule 48.3(b)).
   ☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

   ☐ contained in the international application in written form.
   ☐ filed together with the international application in computer readable form.
   ☐ furnished subsequently to this Authority in written form.
   ☐ furnished subsequently to this Authority in computer readable form.
   ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
   ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

   ☐ the description, pages:
   ☐ the claims, Nos.:
   ☐ the drawings, sheets:

5. ☐ This opinion has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)).

6. Additional observations, if necessary:

V. Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	
Inventive step (IS)	Claims	1-22
Industrial applicability (IA)	Claims	

2. Citations and explanations

see separate sheet

Re Item V

Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. The following documents (D) are mentioned in this written opinion; the numbering will be adhered to in the rest of the procedure.

   D1: WO 02/061510
   D2: US 2002/156898
   D3: WO 02/086724
   D4: WO 02/03653
   D5: US 2002/105910

2. Claim 1 lacks an inventive step (Article 33(3) PCT).

   Document D1, which is considered to represent the most relevant state of the art for claim 1, discloses insofar the subject-matter is clear, according to the subject-matter of claim 1:

   - A method for detecting attacks on a data communications network having a plurality of addresses for assignment to data processing systems in the network (page 6, lines 14-16); the method comprising:
   - identifying data traffic on the network (page 6, lines 22-23);
   - inspecting any data traffic so identified for data indicative of an attack (page 6, lines 30-31); and,
   - on detection of data indicative of an attack, generating an alert signal (page 6, line 31 - page 7, line 2).

   The subject-matter of claim 1 differs from the disclosure in D1 in that:
   - the identified data traffic is originated from any assigned address and addressed to any unassigned address.

   This difference is however without inventive significance for the following reasons:

- the expressions "assigned address" and "unassigned address" are not clear (see point 6.2 below);

- the definition given in the description on page 2, line 27 - page 3, line 5 is not appropriate to clarify the meaning: "The apparatus that is designed to execute the method according to the invention will be the device **those "unassigned" addresses are actually assigned to** in order to make use of the invention. Those addresses are insofar unassigned as they are not assigned to any device that does have another functionality apart from signature generation or intrusion detection". For the examination, this statement for the examination could be interpreted as a honeypot using unassigned addresses, i.e. a standard measure for realising the honeypot being without inventive significance.

3. The above finding also applies to independent claims 8, 15, 16 and 21 which correspond to independent claim 1.

4. Dependent claims do not contain any subject-matter which, in combination with the subject-matter to which they refer, meets the requirements of the PCT in respect of inventive step (Articles 33(3) PCT). They are either disclosed in D2-D5 (e.g. "rerouting any data traffic originating at the address assigned to the data processing system originating the data indicative of the attack to an address on the network", "providing a report to said entity containing information related to one of alert, ...") or common measures (e.g. "the alert message comprises data indicative of the attack detected") obvious for a person skilled in the art.

5. Certain defects in the international application

5.1 The features of the claims are not provided with reference signs place in parentheses (Rule 6.2(b) PCT).

5.2 If new independent claims are filed, these claims should be formulated in the two-part form in accordance with Rule 6.3(b) PCT, with those features known in combination from the prior art document D1 being placed in the preamble (Rule 6.3(b)(I) PCT) and

with the remaining features being included in the characterising part (Rule 6.3(b)(ii) PCT).

If the applicant is of the opinion that the two-part form is not appropriate he is invited to provide reasons in his reply.

5.3 Contrary to the requirements of Rule 5.1(a)(ii) PCT, the relevant background art disclosed in the document D1 is not mentioned in the description, nor is this document identified therein.

5.4 The description should be adapted to any new claims (Rule 5.1(a)(iii) PCT)

5.5 In order to facilitate the examination of the conformity of the amended application with the requirements of Article 19(2) PCT, the applicant is requested to clearly identify the amendments carried out, irrespective of whether they concern amendments by addition, replacement or deletion, and to indicate the passages of the application as filed on which these amendments are based.

6. Certain observations in the international application, i.e. the claims do not meet the requirements of Article 6 PCT:

6.1 Although method claims 1 and 21 and apparatus claims 8 and 15 have been drafted as separate independent claims, they appear to relate effectively to the same subject-matter and to differ from each other only with regard to the definition of the subject-matter for which protection is sought and in respect of the terminology used for the features of that subject-matter. The aforementioned claims therefore lack conciseness.

6.2 The expressions

- "assigned address" and "unassigned address" used in claims 1, 8, and 21;
- "technical data derived for the attack-handling for another of said entities" used in claim 20;
- "the degree of network security achieved" used in claim 19;

- "the turnover of said entity" used in claim 19;

are vague and unclear and leave the reader in doubt as to the meaning of the technical features to which they refer, thereby rendering the definition of the subject-matter of said claims unclear.

6.3 The subject-matter of claims 7, 14, 17 for which protection is sought is not clearly defined. The claims attempt to define the subject-matter in terms of the result to be achieved, which merely amounts to a statement of the underlying problem, without providing the technical features necessary for achieving this result.

6.4 The scope of protection sought for of claim 15 is unclear, since the data communications network is not defined per se but only specified by its relationship to a second entity "a plurality of addresses for assignment to data processing system" and a third entity "apparatus for detecting attacks on the network" and lacks therefore clarity. In addition, there is no link between the second and third entity in order to solve a technical problem.

6.5 The scope of protection sought for of claim 16 is unclear, since it is not clear if the processor is configured to perform all of the method steps or not as claimed in claims 1 to 7.

6.6 An antecedent definition for the expressions

- "the warning message program code" used in claim 7;
- "the warning message" used in claim 14;
- "the charge being billed", "said entity", "the size of the network", "the number of unassigned addresses", the number of assigned addresses", the volume of data traffic", the number of attacks", the number of alerts", "the signature of the identified attack", the volume of rerouted data traffic", "the degree of network security achieved", "the turnover of said entity" used in claim 19;
- "the attack-handling" used in claim 20;

is missing.

6.7 As explained below, some of the features in the apparatus claims 9, 11, 16 relate to a

method of using the apparatus rather than clearly defining the apparatus in terms of its technical features. The intended limitations are therefore not clear from these claims:

- "inspects" in claim 9;
- "sends" in claim 11;
- "configures" used in claim 16.

6.8 The subject-matter of claim 13 is unclear, since it is not clear of how to assign a disinfection server to the disinfection address. However it is clear of how to assign the disinfection address to a disinfection server.

Further unclarity is stemming from the use of the expression "disinfection address" e.g. in claims 3-5 and 13 with different meanings: in claims 3-5 the "disinfection address" is to be understood as "disinfection server".

6.9 The expression "preferably", used in claim 19 leads to doubts about the scope of protection (PCT Guidelines 5.40), because it is unclear if the features following this expression is part of the scope of protection sought for or not.

6.10 The backreference of claim 5 leads to doubts about the scope of protection sought for: said claim is referenced to itself.

6.11 According to Rule 6.4(c) PCT, all claims referring back to a single previous claim, shall be grouped together, which is not the case for claims 17-20, which are referenced back on claim 1.